(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/084459 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 29/06

(21) International Application Number: PCT/US02/11239

(22) International Filing Date: 9 April 2002 (09.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/829,761 10 April 2001 (10.04.2001) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; Paul J. Otterstedt, P.O. Box 218, Yorktown Heights, NY 10598 (US).

(72) Inventors: CHEFALAS, Thomas; 214 Briarwood Drive, Somers, NY 10589 (US). MASTRIANNI, Steven; 15 Great Oak Lane, Unionville, CT 06085 (US). MOHINDRA, Ajay; 1340 Lynn Court, Yorktown Heights, NY 10598 (US).

(74) Agent: YEE, Duke; Carstens, Yee & Cahoon, LLP, P.O. Box 802334, Dallas, TX 75380 (US).

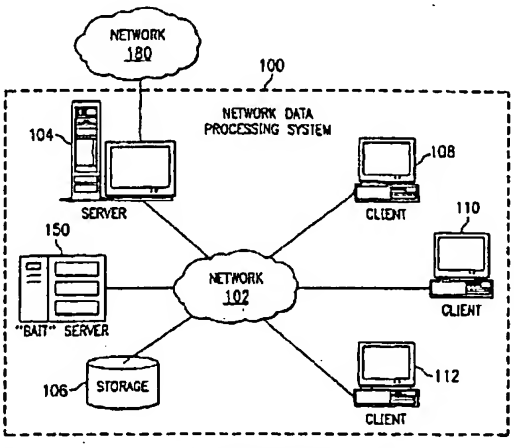
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

[Continued on next page]

(54) Title: DETECTION OF COMPUTER VIRUSES ON A NETWORK USING A BAIT SERVER



(57) Abstract: A method, computer program product, and network data processing system (100) for identifying, locating, and deleting viruses is provided. In one embodiment, the network data processing system (100) includes a local server (104), several client data processing systems (108-112), and a bait server (150). The address of the bait server (150) is not published to the clients (108-112). Thus, any attempt to access the bait server (150) would indicate the presence of a virus on the client attempting access. The bait server (150) monitors itself (408) and, responsive to an attempt from a client to access the bait server (150), broadcasts an indication that a virus attack is underway to all devices within the network. The bait server (150) then ignores all further access requests by the offending client until it receives an indication that the offending client has been disinfected and directs the local server (104) to disconnects the offending client(s) from the network (412). The bait server (150) also notifies the local server and/or a network administrator of the problem and the identity of the offending client allowing appropriate action to be initiated to disinfect the offending client (410).

WO 02/084459 A1

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:
— *with international search report*
— *with amended claims*

Date of publication of the amended claims: 12 December 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AMENDED CLAIMS
[received by the International Bureau on 23 October 2002 (23.10.02);
original claims 1, 10, 13, 16, 20, 23, 26, 30, 33 and 36 amended; remaining claims unchanged (7 pages)]

1. A network data processing system for identifying, locating, and deleting viruses, comprising:

a local server;

a plurality of client data processing systems; and

a bait server having an unpublished network address, wherein

the bait server monitors itself and, responsive to an attempt from an offending system within the network data processing system to access the bait server, the bait server broadcasts an indication that a virus attack is underway to all devices within the network data processing system, ignores all further access requests by the offending system until receiving an indication that the offending system has been disinfected, and directs the local server to disconnect the offending system from the network data processing system.

2. The network data processing system as recited in claim 1, wherein the address of the bait server is not published to the plurality of client data processing systems.

3. The network data processing system as recited in claim 1, wherein the offending system includes more than one data processing system.

4. The network data processing system as recited in claim 1, wherein the offending system includes the local server.

5. The network data processing system as recited in claim 1, wherein the offending system includes a client data processing system.

6. The network data processing system as recited in claim 1, wherein the attempt from the offending system to access the bait server comprises an attempt to write to the bait server.

7. The network data processing system as recited in claim 1, wherein the virus is a worm.

8. The network data processing system as recited in claim 1, wherein the virus is a Trojan horse.

9. The network data processing system as recited in claim 1, wherein the network data processing system is configured to, once the offending system has been disinfected of the client, allow the offending system to reconnect to the network data processing system.

10. A method for detecting the presence of a computer virus, the method comprising;

receiving, at a bait server, a request to perform a function on the bait server, wherein the bait server has an unpublished network address and user access to the bait server is prohibited;

identifying an offending system from which the request originated;

alerting a local server that a virus attack is in progress and of the identity of the offending system; and

directing the local server to disconnect the offending system from the network.

11. The method as recited in claim 10, further comprising:

prior to disconnecting the offending system, notifying the offending system that it is infected with a virus.

12. The method as recited in claim 10, further comprising:

receiving a reconnect request from the offending system;

verifying that the offending system is disinfected and available to reconnect to the network; and

reconnecting the offending system to the network.

13. A method in a bait server for detecting the presence of a computer virus, the method comprising:

monitoring files within the bait server, wherein the bait server has an unpublished address and client access to the bait server is unauthorized; and

responsive to a change in one or more of the files within the bait server, notifying a local server that a virus attack is underway.

14. The method as recited in claim 13, wherein the change in one or more of the files includes a change in byte size of the one or more of the files.

15. The method as recited in claim 13, wherein the change in one or more of the files includes one of a missing and a deleted file.

16. A method in a bait server for detecting the presence of a computer virus, the method comprising:

monitoring, from the bait server, a network for the presence of a computer virus, wherein the bait server has an unpublished network address and access to the bait server by network users is prohibited;

responsive to a determination that a virus is detected, determining the identity of an offending system within the network from which the virus entered the network; and

directing the local server to disconnect the offending system from the network.

17. The method as recited in claim 16, further comprising:

instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication.

18. The method as recited in claim 16, further comprising:

notifying a local server of the presence of the virus and the identify of the offending system.

19. The method as recited in claim 16, further comprising:

responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system, reconnecting the offending system to the network.

20. A computer program product in a computer readable media for use in a data processing system for detecting the presence of a computer virus, the computer program product comprising;

first instructions for receiving, at a bait server, a request to perform a function on the bait server, wherein the bait server has an unpublished network address and user access to the bait server is prohibited;

second instructions for identifying an offending system from which the request originated;

third instructions for alerting a local server that a virus attack is in progress and the identity of the offending system; and

fourth instructions for disconnecting the offending system from a network.

21. The computer program product as recited in claim 20, further comprising:

fifth instructions for, prior to disconnecting the offending system, notifying the offending system that it is infected with a virus.

22. The computer program product as recited in claim 20, further comprising:

fifth instructions for receiving a reconnect request from the offending system;

sixth instructions for verifying that the offending system is disinfected and available to reconnect to the network; and

seventh instructions for reconnecting the offending system to the network.

23. A computer program product in a computer readable media for use in a data processing system in a bait server for detecting the presence of a computer virus, the computer program product comprising:

first instructions for monitoring files within the bait server, wherein the bait server has an unpublished network address and user access to the bait server is prohibited; and

second instructions for responsive to a change in one or more of the files within the bait server, notifying a local server that a virus attack is underway.

24. The computer program product as recited in claim 23, wherein the change in one or more of the files includes a change in byte size of the one or more of the files.

25. The computer program product as recited in claim 23, wherein the change in one or more of the files includes a missing file.

26. A computer program product in a computer readable media for use in a data processing system in a bait server for detecting the presence of a computer virus, the computer program product comprising:

first instructions, in a bait server, for monitoring a network for the presence of a computer virus, wherein the bait server has an unpublished network address and user access to the bait

server is unauthorized;

second instructions, responsive to a determination that a virus is detected, for determining the identity of an offending system within the network from which the virus entered the network; and

third instructions for disconnecting the offending system from the network.

27. The computer program product as recited in claim 26, further comprising:

fourth instructions for instructing all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication.

28. The computer program product as recited in claim 26, further comprising:

fourth instructions for notifying a local server of the presence of the virus and the identify of the offending system.

29. The computer program product as recited in claim 26, further comprising:

fourth instructions, responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, for reconnecting the offending system to the network.

30. A system for detecting the presence of a computer virus, the system comprising;

a receiver, at a bait server, which receives a request to perform a function on the bait serve, wherein the bait server has an unpublished network address and user access to the bait server is unauthorized;

an identifying unit which identifies an offending system from which the request originated;

an virus alert unit which alerts a local server that a virus attack is in progress and the identity of the offending system; and

disconnection unit which disconnects the offending system from a network.

31. The system as recited in claim 30, further comprising:

a notification unit which, prior to disconnecting the offending system, notifies the offending system that it is infected with a virus.

32. The system as recited in claim 30, further comprising:

a reconnect request unit which receives a reconnect request from the offending system;

a verification unit which verifies that the offending system is authorized to reconnect to the network; and

a reconnecting unit which reconnects the offending system to the network.

33. A system in a bait server for detecting the presence of a computer virus, the system comprising:

a monitoring unit which monitors files within the bait server, wherein the bait server has an unpublished network address and wherein user access to the bait server is unauthorized; and

a notification unit which, responsive to a change in one or more of the files within the bait server, notifies a local server that a virus attack is underway.

34. The system as recited in claim 33, wherein the change in one or more of the files includes a change in byte size of the one or more of the files.

35. The system as recited in claim 33, wherein the change in one or more of the files includes a missing file.

36. A system in a bait server for detecting the presence of a computer virus, the system comprising:

a monitoring unit, in a bait server, which monitors a network for the presence of a computer virus, wherein the bait server has an unpublished network address and user access to the bait server is unauthorized;

an identifier which, responsive to a determination that a virus is detected, determines the identity of an offending system within the network from which the virus entered the network; and

a disconnection unit which disconnects the offending system from the network.

37. The system as recited in claim 36, further comprising:

a network protection unit which instructs all devices within the network to ignore all requests from the offending system until the offending system is reauthorized for network communication.

38. The system as recited in claim 36, further comprising:

a notification unit which notifies a local server of the presence of the virus and the identify of the offending system.

39. The system as recited in claim 36, further comprising:

a reconnection unit which, responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system, reconnects the offending system to the network.